Bitdefender

GravityZone 商业版

GravityZone 商业版 适合预算有限的小型企业，提供基础的安全防护，可保护Windows，Linux和macOS等各类系统，PC和服务器等。

“Bitdefender阻止了100%的零日恶意软件和在野威胁。”

AV-TEST首席执行官Maik Morgenstern评价： “ Bitdefender每年都在测试时证明了其卓越性和可靠性。” “在2020年，Bitdefender发光得比以往任何时候都要亮。凭借四项最佳保护大奖，Bitdefender展示了其在市场上的至高无上的地位。在针对企业用户，以及个人用户和移动产品的测试中，Bitdefender出色的保护力给我们留下了深刻的印象。”

— “AV-Test 2020 年度最佳保护产品”
— “AV-Comparatives 2020 年度卓越产品”

主要功能

世界排名第一的反病毒技术，国际权威机构测评，连续10年排名第一

BitDefender连续多年在国际权威测评机构AV-Test和AV-Comparatives的测试中排名第一，始终如一的卓越保护，值得信赖。我们的客户包括：奇虎360，腾讯，百度，阿里巴巴，华为，电讯盈科，Microsoft，Cisco，IBM, FireEye等等。

人工智能和机器学习反恶意软件

Bitdefender高级人工智能和机器学习技术使用超过80000+模型，40000多种静态和动态功能，它们不断接受来自全球5亿个端点的数万亿个样本的训练，这确保了GravityZone在恶意软件检测方面的全球领先性，提前预测攻击并应对网络犯罪的增长。

高级威胁防护 基于零信任持续监控进程行为

高级威胁防护以零信任模式运行，持续监控操作系统中运行的所有进程。 它可以捕获可疑活动或异常进程行为，例如尝试伪装进程类型，在另一个进程的空间中执行代码（劫持进程内存以进行权限提升），复制，删除文件，隐藏进程，枚举应用程序等等。 它可以自动采取适当的处理措施，包括终止进程和撤消进程所做的系统修改。 它在检测未知高级恶意软件（包括勒索病毒）方面非常有效。

Bitdefender

勒索病毒免疫

该解决方案基于全球超过5亿个终端的高级威胁情报。 无论恶意软件出现在什么地方，增加多少，Bitdefender都可快速检测，将其入库，为全球用户提供勒索免疫疫苗，免疫勒索病毒。

勒索病毒缓解 自动恢复被勒索病毒加密的文件

凭借强大的主动防护和屡获殊荣的检测技术，勒索病毒缓解提供了一种针对未知勒索病毒攻击的主动解决方案。 勒索缓解技术会实时检测攻击，将其立即阻止，无论它是在本地运行还是从远程端点运行，然后自动恢复攻击前期被加密的文件。

网络攻击防护

防止攻击者利用网络漏洞来访问系统，进行横向移动。全面拦截RDP和SSH暴力破解攻击，端口扫描，Samba攻击，服务漏洞攻击，窃取密码，网络漏洞利用，SQL注入攻击，目录遍历，僵尸网络攻击，恶意网址，远程IoT攻击，TOR/Onion连接等等。

高级反漏洞利用

高级反漏洞利用技术可保护系统内存和易受攻击的应用程序，防止未经授权的进程提升权限和访问资源，保护LSASS进程免于泄露密码哈希和安全设置等。预先配置了常用列表，如浏览器，文档阅读器，媒体文件和运行时（即Flash，Java）。 高级机制监视内存访问机制，以检测和阻止已知和位置的漏洞利用技术，如API调用验证，堆栈透视，ShellCode，Meterpreter, 返回导向编程（ROP）等。 GravityZone的反漏洞利用技术可以拦截先进的，隐蔽的渗透攻击，APT攻击等，全面保护你的基础设施安全。

5亿用户全球最大的安全情报云

Bitdefender拥有全球最大的云安全网络，5亿用户遍布全球。使用最先进的AI和机器学习算法来捕获最新的网络威胁，每天执行110亿次安全查询。100亿海量样本训练，能够精准识别零日威胁，漏洞攻击，定向攻击，高持续威胁攻击，灰色软件，勒索病毒，网络流量攻击，可在短短3秒内实时检测、预防、查杀全球最新的网络威胁。

风险管理 修复系统配置错误

系统配置错误是导致大规模安全灾难的第二大原因，大多数威胁针对众所周知的应用程序和配置漏洞。Bitdefender内置的风险分析引擎不断计算端点的风险评分，以便你轻松对资产进行排序和优先级排序，优先考虑数百个指标的风险严重性和提供安全补救措施。帮助您自动/手动配置Windows安全基线，减少浏览器，操作系统和网络的攻击面。

自动回滚恶意软件对系统的更改

一旦检测到威胁，GravityZone会立即自动采取操作，包括结束进程，隔离，删除, 回滚恶意软件对系统的更改等。 它与Bitdefender全球云安全系统实时共享威胁信息，以防止全球范围内的类似攻击。

主机安全加固

基于策略的端点控制和安全加固包括一系列的技术，例如：防火墙，可屏蔽端口扫描，CC通讯，反弹shell通讯，屏蔽攻击者常用的网络漏洞利用端口135，137，138，139，445端口，设备控制以及具有URL分类的Web访问控制，应用程序控制等，IT管理员可添加攻击者常用的系统进程到黑名单，拒绝其在网络中运行，增强安全等级，

例如，添加阻止规则：autoit.exe, bitsadmin.exe, cscript.exe, java.exe, javaw.exe, miprvse.exe, net.exe,netsh.exe, powershell.exe, powershell_ise.exe, py.exe, python.exe, regedit.exe, regsvr32.exe,rundll32.exe, schtasks.exe, 和 wscript.exe 等等。

Web安全防护

Web安全过滤可实现对传入Web流量的实时扫描，包括SSL，http和https流量，以防止恶意软件下载到端点。 反网络钓鱼保护可自动阻止网络钓鱼和欺诈性网页。

漏洞扫描和补丁管理

未打补丁的系统使组织容易受到黑客攻击，感染病毒和数据泄露。 GravityZone补丁管理可帮助您在整个Windows基础上保持操作系统和应用程序的最新状态 – 支持工作站，物理服务器和虚拟服务器。 它作为独立的安全插件提供。

全盘加密 保护数据安全

GravityZone全盘加密使用原生的Windows BitLocker和Mac FileVault，利用操作系统内置的技术，提供了最好的兼容性，并集成于杀毒软件中，无需安装额外的客户端程序和密钥管理服务器。 它作为独立的安全插件提供。

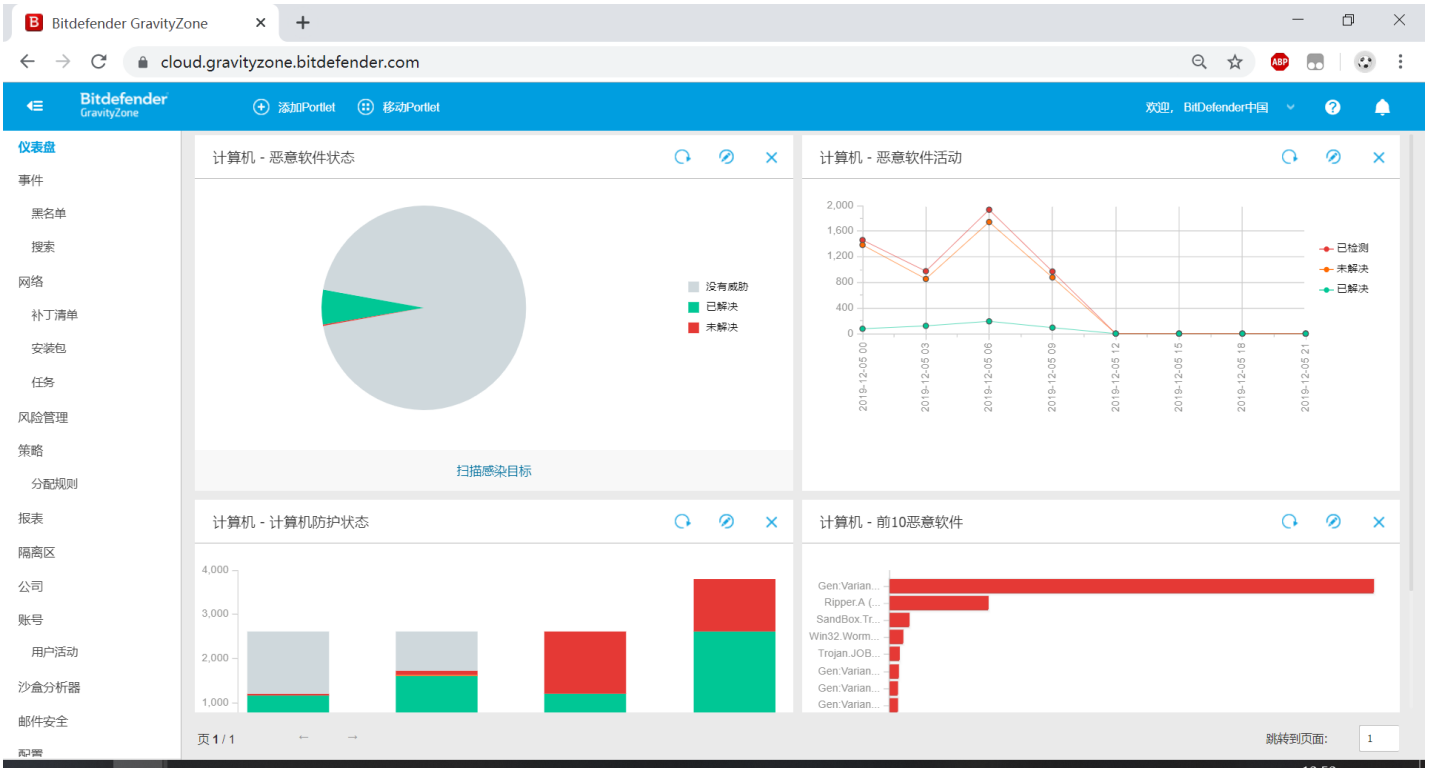
安全技术堆栈

GravityZone提供了世界顶级的安全堆栈，从系统安全加固、预防、检测和响应等多个维度，集成了35+安全防护层，阻止99.9%+的恶意软件和零日威胁。

Bitdefender

管理控制台

管理控制台是一个集中的管理中心，可为所有安全管理组件提供单一窗格视图，您可以在一个控制台中全面管理所有的设备：PC，服务器。管理控制台还提供灵活的选择，你可以选择SaaS云控制台（非常小型企业或跨区域、跨全球的超大型企业），或者，您也可以将控制台部署在单位内部，进行精细化的安全管理。



Bitdefender

Bitdefender的优势

世界顶级的安全能力，极低的资源占用，易于使用

AV-Test CEO评价： “Bitdefender每年都在测试时证明了其卓越性和可靠性。” “在2020年，Bitdefender发光得比以往任何时候都要亮。凭借四项最佳保护产品大奖，Bitdefender展示了其在市场上的至高无上的地位。在针对企业用户，以及个人用户和移动产品的测试中，Bitdefender出色的保护力给他们留下了深刻的印象。” Bitdefender阻止了100%的零日恶意软件和在野威胁。 “

- 部署非常方便，可选择使用SaaS云控制台，或本地私有化部署。SaaS控制台登陆即可使用，无需准备服务器资源部署控制台。
- 一个控制台集中管理所有设备，Windows，Linux，Mac OS等
- 世界顶级的安全保护能力
- 极低的资源占用，安装后即可忘记它，你甚至感觉不到它的存在
- 支持整个架构的全自动更新，您可以充分享受BitDefender推出的更新和功能改进等，不用担心跨版本升级需要重装客户端的问题。

欲了解更多，请访问官网产品页面: http://www.bitdefender-cn.com/business/smb-products/business-security.html

扫码关注Bitdefender微信公众号

每周获取最新的安全资讯、知识与经验，促销活动等

立即体验 **GravityZone Business Security** 吧! 我们提供免费试用，立即申请:

http://www.bitdefender-cn.com/trial.html

联系销售部门:

4000-132-568 sales@bitdefender-cn.com

Bitdefender

Bitdefender是一家全球领先的网络安全技术公司，为150多个国家的5亿用户提供尖端的端到端网络安全解决方案和先进的威胁防护，全球超过38%的安全公司使用Bitdefender的技术,例如：奇虎360，腾讯，百度，阿里巴巴，Microsoft，Cisco， IBM, FireEye，GDATA等等。自2001年以来，Bitdefender一直致力于开发屡获殊荣的商业和消费者安全技术，并且是混合基础设施安全和端点保护的首选供应商。

All Rights Reserved. © 2021 Bitdefender. All trademarks, trade names, and products referenced herein are property of their respective owners.